

OPAM-OIM Integration

How to integrate OPAM to work in tandem with OIM?

Software versions

OPAM - 11g R2 PS2

OIM - 11g R2 PS2

Assumptions: OIM is installed as a part of the Oracle IDAM R2 PS2 suite

Note: OPAM is installed in a separate Weblogic domain than that of OIM

Why integrate OIM and OPAM?

OPAM-OIM integration is primarily done so that ***the access to privilege accounts*** via OPAM can be ***regulated through OIM***.

OIM can be ***integrated with the LDAP Identity Store using LDAP Connector or LDAPSsync*** and end users can be subjected to an ***request based approval workflow*** in order to get access to certain ***LDAP groups*** in the OPAM Identity Store. These ***LDAP groups in turn can be configured within OPAM*** for managing secure access to Privileged accounts and targets.

1. Configure the Identity Store for OPAM

We are going to use Apache DS LDAP server as an example.

We will configure Apache DS as

- ***Identity Store for OPAM*** - an appropriate ***Authentication Provider*** will be configured in OPAM Weblogic Admin console (this will ***replace the Weblogic Embedded LDAP*** used in previous examples)
- ***Managed Target within OIM*** - integrated via ICF LDAP Connector

ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: opam_domain

Home > Summary of Security Realms

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

Realms (Filtered - More Columns Exist)

New	Delete	Showing 1 to 1 of 1 Previous Next	
<input type="checkbox"/>	Name	Default Realm	
<input type="checkbox"/>	myrealm	true	
New	Delete	Showing 1 to 1 of 1 Previous Next	

Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: opam_domain

Home > Summary of Security Realms > myrealm > Providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

[Customize this table](#)

Authentication Providers

New	Delete	Reorder	Showing 1 to 3 of 3 Previous Next	
<input type="checkbox"/>	Name	Description	Version	
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0	
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0	
<input type="checkbox"/>	TrustServiceIdentityAsserter	Trust Service Identity Assertion Provider	1.0	

Create a New Authentication Provider

OK

Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

The name of the authentication provider.

* Name:

This is the type of authentication provider you wish to create.

Type:

OK

Cancel

Settings for myrealm

[Configuration](#) [Users and Groups](#) [Roles and Policies](#) [Credential Mappings](#) **Providers** [Migration](#)**Authentication** [Password Validation](#) [Authorization](#) [Adjudication](#) [Role Mapping](#) [Auditing](#) [Credential Mapping](#) [Certification Path](#) [Keystores](#)

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

[Customize this table](#)

Authentication Providers

NewDeleteReorder

Showing 1 to 4 of 4PreviousNext

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	TrustServiceIdentityAsserter	Trust Service Identity Assertion Provider	1.0
<input type="checkbox"/>	LDAPAuthenticationProvider	Provider that performs LDAP authentication	1.0

NewDeleteReorder

Showing 1 to 4 of 4PreviousNext

Home Log Out Preferences Record Help Welcome, weblogic Connected to: opam_dor

Home > Summary of Security Realms > myrealm > Providers > LDAPAuthenticationProvider

Settings for LDAPAuthenticationProvider

Configuration Performance

Common Provider Specific

Save

This page displays basic information about this LDAP Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequence.

Name:	LDAPAuthenticationProvider	The name of the Java class used to load the LDAP Authentication provider. More Info...
Description:	Provider that performs LDAP authentication	A short description of the LDAP Authentication provider. More Info...
Version:	1.0	The version number of the LDAP Authentication provider. More Info...
Control Flag:	SUFFICIENT	Returns how the login sequence uses the Authentication provider. More Info...

Save

Configuration Performance

Common Provider Specific

Save

Use this page to define provider specific configuration for this LDAP Authentication provider.

Connection

Host:	192.168.1.101	The host name or IP address of the LDAP server. More Info...
Port:	10389	The port number on which the LDAP server is listening. More Info...
Principal:	uid=admin,ou=system	The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. More Info...
Credential:	The credential (usually a password) used to connect to the LDAP server. More Info...
Confirm Credential:	

☐ SSL Enabled Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#)

Users

User Base DN:	dc=thentbigthing,dc=c	The base distinguished name (DN) of the tree in the LDAP directory that contains users. More Info...
All Users Filter:		If the attribute (user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. More Info...
User From Name Filter:	.u)(objectclass=person))	If the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. More Info...

User Search Scope:	subtree ▼	Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. More Info...
User Name Attribute:	uid	The attribute of an LDAP user object that specifies the name of the user. More Info...
User Object Class:	person	The LDAP object class that stores users. More Info...
<input type="checkbox"/> Use Retrieved User Name as Principal Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. More Info...		
Groups		
Group Base DN:	ou=entGroups,dc=thene:	The base distinguished name (DN) of the tree in the LDAP directory that contains groups. More Info...
All Groups Filter:		An LDAP search filter for finding all groups beneath the base group distinguished name (DN). If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the Group schema. More Info...
Group From Name Filter:	=groupofuniquenames))	An LDAP search filter for finding a group given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. More Info...
Group Search Scope:	subtree ▼	Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. More Info...
Group Membership Searching:	unlimited ▼	Specifies whether group searches into nested groups are unlimited or limited. Valid values are unlimited and limited. More Info...
Max Group Membership Search Level:	0	Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of levels to search. More Info...

..... Leave all the other default values except for the ones which are highlighted

Reorder the provider

Settings for myrealm

Configuration
Users and Groups
Roles and Policies
Credential Mappings
Providers
Migration

Authentication
Password Validation
Authorization
Adjudication
Role Mapping
Auditing
Credential Mapping
Certification Path
Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

[Customize this table](#)

Authentication Providers

New
Delete
Reorder

Showing 1 to 4 of 4
Previous
Next

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	TrustServiceIdentityAsserter	Trust Service Identity Assertion Provider	1.0
<input type="checkbox"/>	LDAPAuthenticationProvider	Provider that performs LDAP authentication	1.0

New
Delete
Reorder

Showing 1 to 4 of 4
Previous
Next

Reorder Authentication Providers

OK

Cancel

Reorder Authentication Providers

You can reorder your Authentication Providers using the list below. By reordering Authentication Providers, you can alter the authentication sequence.

Select authenticator(s) in the list and use arrows to move them up and down in the list.

Authentication Providers:

Available:

☐ DefaultAuthenticator
 ☐ DefaultIdentityAsserter
 ☐ TrustServiceIdentityAsserter
 ☒ LDAPAuthenticationProvider

Move selected items up in list

OK

Cancel

Reorder Authentication Providers

OK

Cancel

Reorder Authentication Providers

You can reorder your Authentication Providers using the list below. By reordering Authentication Providers, you can alter the authentication sequence.

Select authenticator(s) in the list and use arrows to move them up and down in the list.

Authentication Providers:

Available:

☒ LDAPAuthenticationProvider
 ☐ DefaultAuthenticator
 ☐ DefaultIdentityAsserter
 ☐ TrustServiceIdentityAsserter

OK

Cancel

Customize this table

Authentication Providers

New

Delete

Reorder

Showing 1 to 4 of 4 Previous | Next

<input type="checkbox"/>	Name	Description	Version
<input checked="" type="checkbox"/>	LDAPAuthenticationProvider	Provider that performs LDAP authentication	1.0
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	TrustServiceIdentityAsserter	Trust Service Identity Assertion Provider	1.0

New

Delete

Reorder

By Abhishek Gupta

Change Control Flag for Default Authenticator from REQUIRED to SUFFICIENT

Home > Summary of Security Realms > myrealm > Providers > LDAPAuthenticationProvider > Summary of Security Realms > myrealm > Providers > DefaultAuthenticator

Settings for DefaultAuthenticator

Configuration Performance Migration

Common Provider Specific

Save

This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequence.

Name:	DefaultAuthenticator	The name of this WebLogic Authentication provider. More Info...
Description:	WebLogic Authentication Provider	A short description of the Authentication provider. More Info...
Version:	1.0	The version number of the Authentication provider. More Info...
Control Flag:	<div>REQUIRED REQUIRED REQUISITE SUFFICIENT OPTIONAL</div>	Returns how the login sequence uses the Authentication provider. More Info...

Save

Settings for DefaultAuthenticator

Configuration Performance Migration

Common Provider Specific

Save

This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequence.

Name:	DefaultAuthenticator	The name of this WebLogic Authentication provider. More Info...
Description:	WebLogic Authentication Provider	A short description of the Authentication provider. More Info...
Version:	1.0	The version number of the Authentication provider. More Info...
Control Flag:	SUFFICIENT	Returns how the login sequence uses the Authentication provider. More Info...

Save

Restart Weblogic Admin and OPAM Managed Server

Note: On starting Weblogic Admin server, you might receive the below error



opam-weblogic-admin-server-error.txt

Do the following

Take a backup of your config.xml (OPAM_DOMAIN/config)



Change it as per below snapshot

```
<domain-version>10.3.6.0</domain-version>
<security-configuration>
  <name>opam_domain</name>
  <realm>
    <sec:authentication-provider xsi:type="wls:open-ldap-authenticatorType">
      <sec:name>LDAPAuthenticationProvider</sec:name>
      <sec:control-flag>SUFFICIENT</sec:control-flag>
      <wls:host>192.168.1.101</wls:host>
      <wls:port>10389</wls:port>
      <wls:principal>uid=admin,ou=system</wls:principal>
      <wls:user-base-dn>ou=employees,dc=thenextbigthing,dc=com</wls:user-base-dn>
      <wls:credential-encrypted>{AES}VdpAgcG6HBjYdIX2GVyfWq1KFcuS07efChV4w8NcwHI=</wls:credential-encrypted>
      <wls:group-base-dn>ou=entGroups,dc=thenextbigthing,dc=com</wls:group-base-dn>
    </sec:authentication-provider>
  </realm>
</security-configuration>
```

Start the Admin server again

Start the OPAM Managed Server after that

Sanity checks

Check user and groups in Weblogic Admin Console

Home > Summary of Security Realms > myrealm > Realm Roles > Users and Groups

Settings for myrealm

ConfigurationUsers and GroupsRoles and PoliciesCredential MappingsProvidersMigration

UsersGroups

This page displays information about each user that has been configured in this security realm.

[Customize this table](#)

Users

NewDelete

Showing 1 to 10 of 27PreviousNext

<input type="checkbox"/>	Name ↕	Description	Provider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	emp101 emp101		LDAPAuthenticationProvider
<input type="checkbox"/>	emp102		LDAPAuthenticationProvider
<input type="checkbox"/>	emp102F emp102L		LDAPAuthenticationProvider
<input type="checkbox"/>	emp103F emp103L		LDAPAuthenticationProvider
<input type="checkbox"/>	emp104		LDAPAuthenticationProvider
<input type="checkbox"/>	emp104		LDAPAuthenticationProvider

NewDelete

Showing 1 to 10 of 27PreviousNext

UsersGroups

This page displays information about each group that has been configured in this security realm.

[Customize this table](#)

Groups

NewDelete

Showing 1 to 10 of 16PreviousNext

<input type="checkbox"/>	Name ↕	Description	Provider
<input type="checkbox"/>	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
<input type="checkbox"/>	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
<input type="checkbox"/>	App1Access		LDAPAuthenticationProvider
<input type="checkbox"/>	App2Access		LDAPAuthenticationProvider
<input type="checkbox"/>	App3Access		LDAPAuthenticationProvider
<input type="checkbox"/>	AppTesters	AppTesters group.	DefaultAuthenticator
<input type="checkbox"/>	CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
<input type="checkbox"/>	Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
<input type="checkbox"/>	Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
<input type="checkbox"/>	oimusers		LDAPAuthenticationProvider

NewDelete

Showing 1 to 10 of 16PreviousNext

Log into OPAM using user credentials from LDAP (we'll use the user which is highlighted below)

<input type="checkbox"/>	Name	Description	Provider
	demouser demouser 123		LDAPAuthenticationProvider
	demouser demouser 123		LDAPAuthenticationProvider
	demouser demouser 123		LDAPAuthenticationProvider
	demouser demouser 123		LDAPAuthenticationProvider
	emp101 emp101		LDAPAuthenticationProvider
	emp102		LDAPAuthenticationProvider
	emp102F emp102L		LDAPAuthenticationProvider
	emp103F emp103L		LDAPAuthenticationProvider
	emp104		LDAPAuthenticationProvider
	emp104		LDAPAuthenticationProvider

ORACLE Privileged Account Manager About Oracle

Sign In

Oracle Privileged Account Manager

User ID

Password

Sign In

ORACLE Privileged Account Manager Accessibility Help Sign Out emp101 emp101

Home

- My Accounts
- My Checkouts

My Accounts

Search Accounts

Account Name Domain

Target Type Description

Target Name

Search **Reset**

Search Results

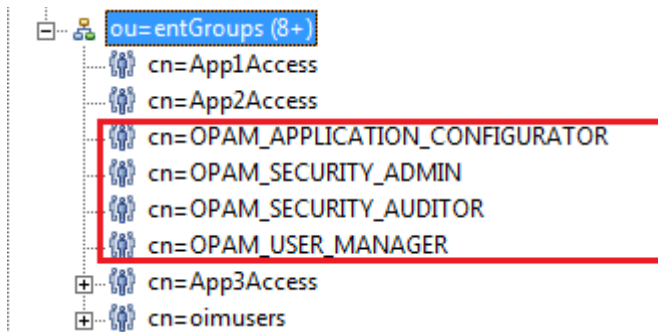
Actions

Row	Account Name	Target Name	Target Type	Domain	Description
No accounts found.					

Create corresponding LDAP Roles in your Identity Store to map to the OPAM Admin Roles

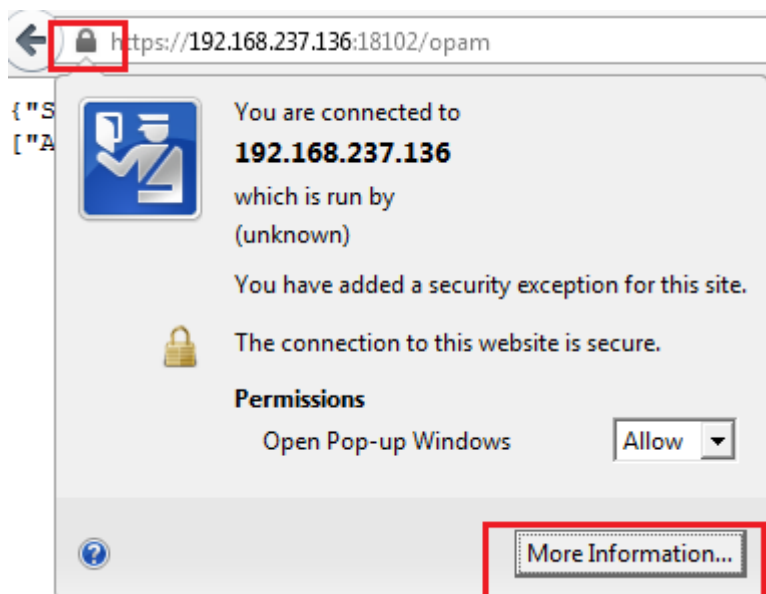
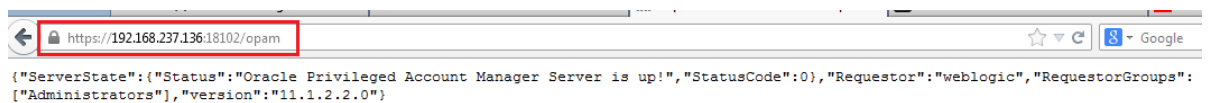
(Follow exact names as provided in

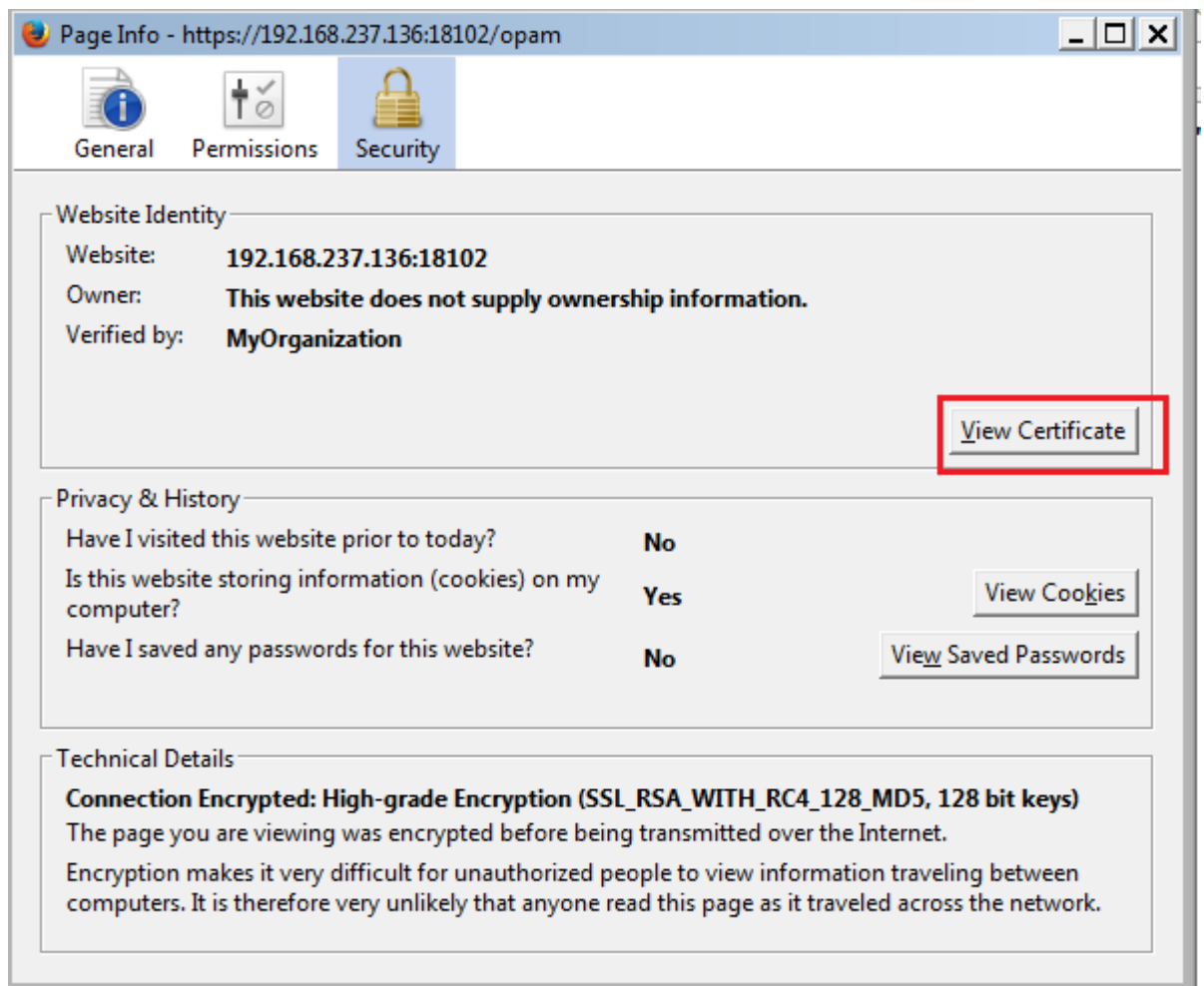
http://docs.oracle.com/cd/E40329_01/admin.1112/e27152/und_security.htm#BGBFHEFC)

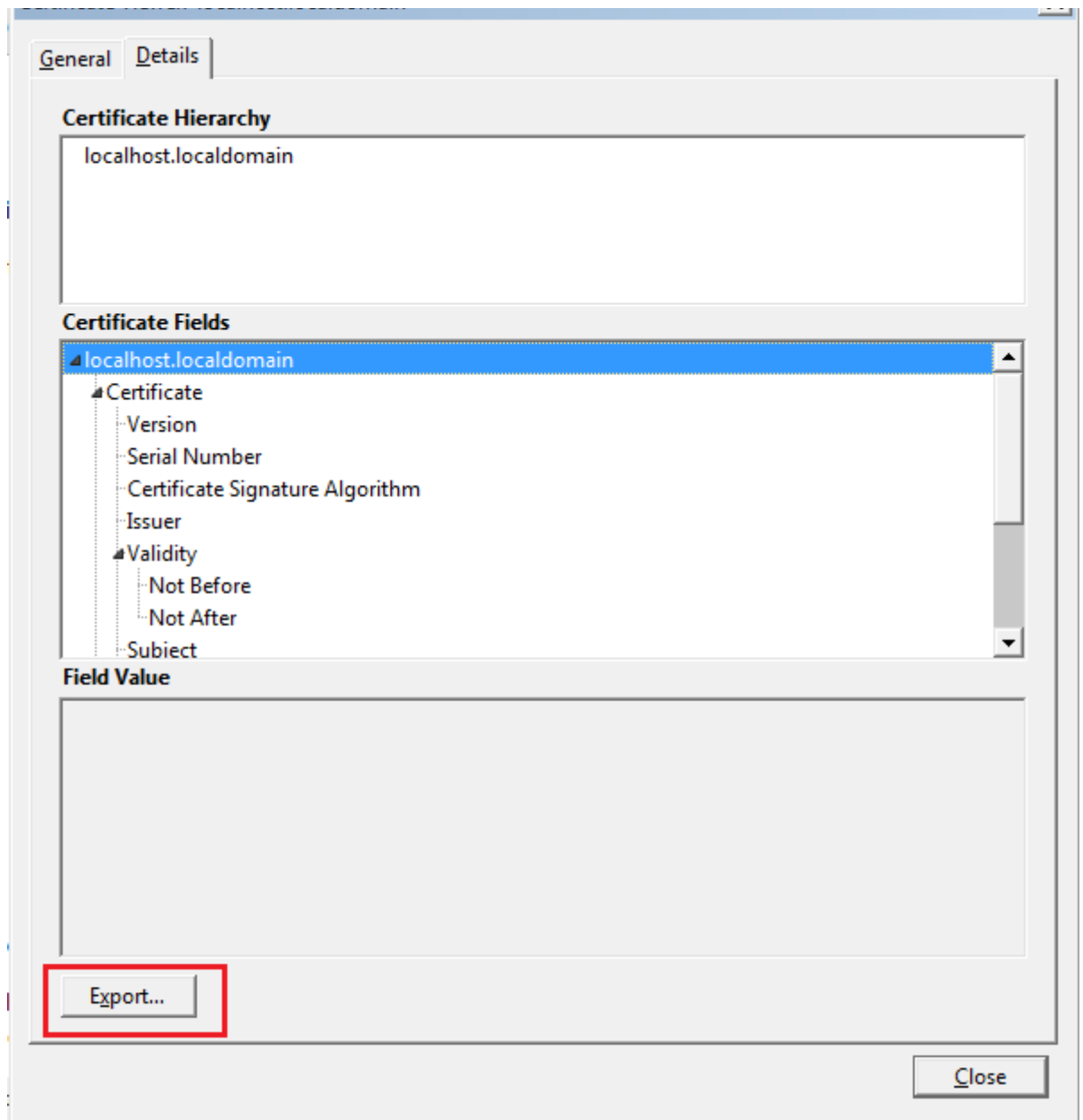


2. Add the OPAM CA certificate in OIM's Weblogic TrustStore in order for ***OIM to be able to call OPAM web services***

Access OPAM Server







Save it on the OPAM machine



Import the same in to the JDK which your OPAM weblogic server

Note: Please take a backup if your original Truststore

```
oracle@localhost:/u01/jdk1.7.0_45/jre/lib/security
File Edit View Terminal Tabs Help
[oracle@localhost ~]$ cd /u01/jdk1.7.0_45/jre/lib/security
[oracle@localhost security]$ cp cacerts cacerts.bkp.20140415
[oracle@localhost security]$
```

***keytool -import -file /u01/OPAMServerCert.pem -keystore
/u01/jdk1.7.0_45/jre/lib/security/cacerts -storepass changeit -alias OPAMServerCert***

```
File Edit View Terminal Tabs Help
[oracle@localhost bin]$ keytool -import -file /u01/OPAMServerCert.pem -keystore /u01/jdk1.7.0_45/jre/lib/security/cacerts -
storepass changeit -alias OPAMServerCert
Owner: CN=localhost.localdomain, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown, ST=MyState, C=US
Issuer: CN=CertGenCAB, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown, ST=MyState, C=US
Serial number: -31335aafac90e28419dd26176a5b895
Valid from: Mon Jan 20 15:38:48 IST 2014 until: Sun Jan 21 15:38:48 IST 2029
Certificate fingerprints:
    MD5: 32:CC:A5:CD:1E:56:CB:A2:AC:A1:C1:D1:13:28:F4:B6
    SHA1: E3:6B:0F:26:76:45:C5:28:74:F8:2A:2A:50:AE:83:77:06:A8:77:27
    SHA256: BA:93:F0:1F:32:40:3E:F7:F3:29:73:BC:54:A3:E1:54:19:F0:BF:78:BE:0C:A6:55:66:D8:B1:B9:9A:49:6B:5A
Signature algorithm name: MD5withRSA
Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
[oracle@localhost bin]$
```

Confirm the same

keytool -list -keystore /u01/jdk1.7.0_45/jre/lib/security/cacerts -storepass changeit -alias OPAMServerCert

```
oracle@localhost:/u01/jdk1.7.0_45/jre/bin
File Edit View Terminal Tabs Help
[oracle@localhost bin]$ keytool -list -keystore /u01/jdk1.7.0_45/jre/lib/security/cacerts -storepass changeit -alias OPAMSe
rverCert
OPAMServerCert, Apr 15, 2014, trustedCertEntry,
Certificate fingerprint (SHA1): E3:6B:0F:26:76:45:C5:28:74:F8:2A:2A:50:AE:83:77:06:A8:77:27
[oracle@localhost bin]$
```


3. Create an OPAM Admin account

Create a user in LDAP (Apache) who you want to assign as the OPAM Admin

DN: uid=apacheopamadmin,ou=employees,dc=thenextbigthing,dc=com	
Attribute Description	Value
<i>objectClass</i>	<i>inetOrgPerson (structural)</i>
<i>objectClass</i>	<i>organizationalPerson (structural)</i>
<i>objectClass</i>	<i>person (structural)</i>
<i>objectClass</i>	<i>top (abstract)</i>
cn	apacheopamadmin
sn	opamadmin
givenname	DEMOUSERF_U
mail	apacheopamadmin@testmail.com
uid	apacheopamadmin
userPassword	SSHA hashed password

Users

[New](#) [Delete](#)

<input type="checkbox"/>	Name 	Description	Provider
<input type="checkbox"/>	apacheopadmin		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	demouser demouser 123		LDAPAuthenticationProvider
<input type="checkbox"/>	emp101 emp101		LDAPAuthenticationProvider
<input type="checkbox"/>	emp102		LDAPAuthenticationProvider
<input type="checkbox"/>	emp102F emp102L		LDAPAuthenticationProvider
<input type="checkbox"/>	emp103F emp103L		LDAPAuthenticationProvider
<input type="checkbox"/>	emp104		LDAPAuthenticationProvider

Log into the OINAV console to assign OPAM specific Admin Roles

ORACLE Identity Navigator About Oracle

Sign In

Oracle Identity Navigator

User ID

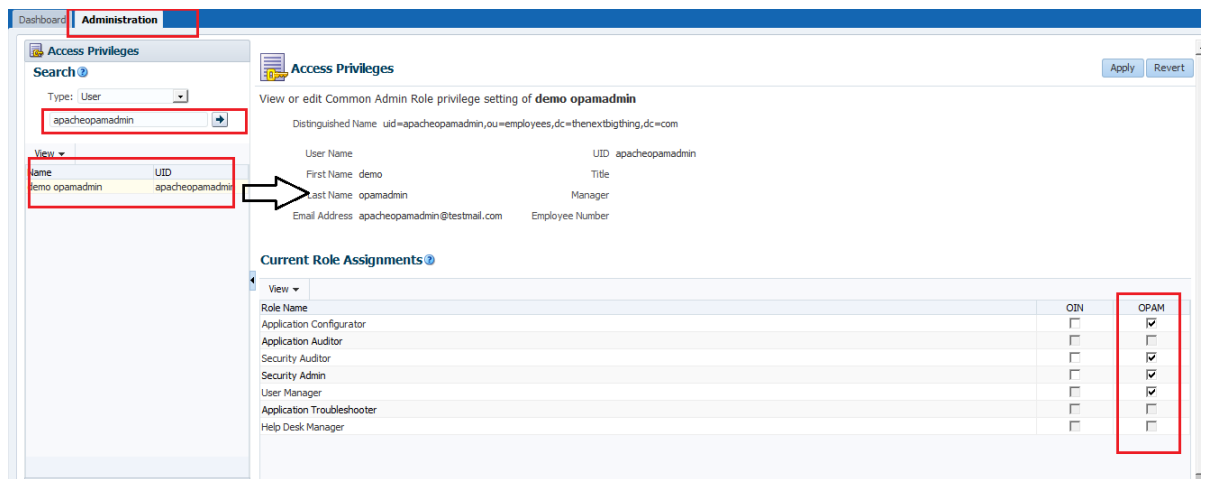
weblogic

Password

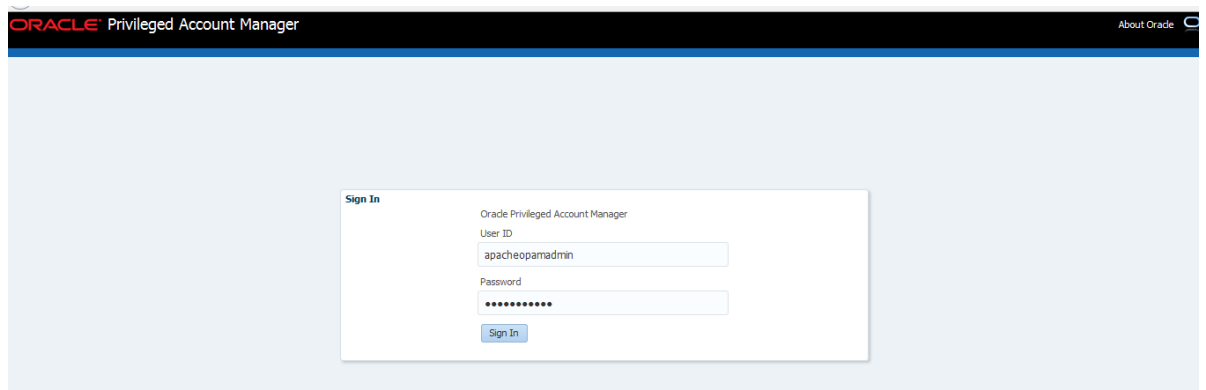
••••••••••

[Sign In](#)

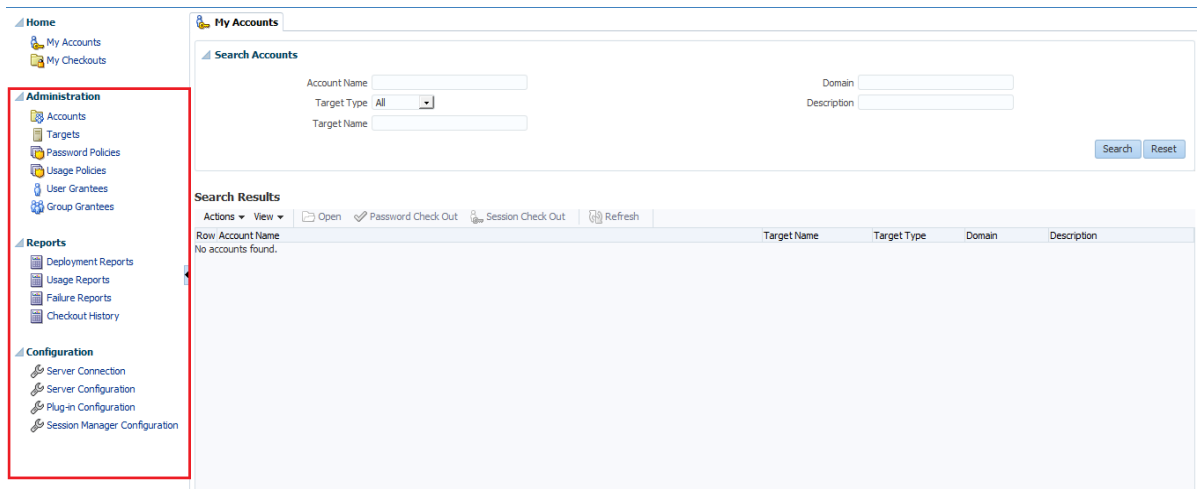
Provide all the OPAM Admin Roles



Log into OPAM with the user to confirm



He has all the authorization as per Admin Roles



4. Run **opamSetup** script

```
export APP_SERVER=weblogic
```

```
export OIM_ORACLE_HOME=/u01/Oracle/Middleware/Oracle_IDM1
```

```
export MW_HOME=/u01/Oracle/Middleware
```

```
export WL_HOME=/u01/Oracle/Middleware/wlserver_10.3
```

```
export DOMAIN_HOME=/u01/Oracle/Middleware/user_projects/domains/oim_domain
```

```
cd /u01/Oracle/Middleware/Oracle_IDM1/server/bin
```

```
./opamSetup.sh
```

```
oracle@localhost:/u01/Oracle/Middleware/Oracle_IDM1/server/bin
File Edit View Terminal Tabs Help
[oracle@localhost bin]$ export APP_SERVER=weblogic
[oracle@localhost bin]$ export OIM_ORACLE_HOME=/u01/Oracle/Middleware/Oracle_IDM1
[oracle@localhost bin]$ export MW_HOME=/u01/Oracle/Middleware
[oracle@localhost bin]$ export WL_HOME=/u01/Oracle/Middleware/wlserver_10.3
[oracle@localhost bin]$ export DOMAIN_HOME=/u01/Oracle/Middleware/user_projects/domains/oim_domain
[oracle@localhost bin]$ pwd
/u01/Oracle/Middleware/Oracle_IDM1/server/bin
[oracle@localhost bin]$ ./opamSetup.sh
```

Start entering details as prompted

```
INFO: OPAM-OIM integration setup script.
Enter OIM URL (t3://oimhost:oimport for weblogic or corbaloc:iiop:oimhost:oimport for websphere) ::t3://localhost:14000
Enter OIM username :xelsysadm
Enter OIM user password :
Enter OPAM IT resource name :OPAMServer
Enter OPAM server name :localhost
Enter OPAM server port :18102
Enter OPAM user :apacheopamadmin
Enter OPAM user password :
Enter ID Store IT resource name :Apache DS LDAP
Enter Context (weblogic.jndi.WLInitialContextFactory for weblogic or com.ibm.websphere.naming.WsnInitialContextFactory for websphere) :[weblogic.jndi.WLInitialContextFactory] weblogic.jndi.WLInitialContextFactory
```

```
Enter ID Store IT resource name :Apache DS LDAP
Enter Context (weblogic.jndi.WLInitialContextFactory for weblogic or com.ibm.websphere.naming.WsnInitialContextFactory for websphere) :[weblogic.jndi.WLInitialContextFactory] weblogic.jndi.WLInitialContextFactory
Apr 15, 2014 8:03:52 PM oracle.iam.opamintg.setup.SetupOIMOPAMIntg setSystemFlag
INFO: system property OIM.OPAM.Integration created successfully.
Apr 15, 2014 8:03:55 PM oracle.iam.opamintg.setup.SetupOIMOPAMIntg createOpamItResource
INFO: IT Resource OPAMServer created successfully.
Apr 15, 2014 8:03:57 PM oracle.iam.opamintg.setup.SetupOIMOPAMIntg createUDF
INFO: UDF column created successfully
Apr 15, 2014 8:03:58 PM oracle.iam.opamintg.setup.SetupOIMOPAMIntg createJob
INFO: Scheduled job OPAM Catalog Synchronization created successfully.
[oracle@localhost bin]$
```

Confirm the artifacts on OIM end

Log into OIM

Check System Property

Welcome **System Property Detail: Enable OIM-OPAM Integration**

System Property Detail: Enable OIM-OPAM Integration

* Key

* Property Name

* Keyword

* Value

Log In Required ☒

Check IT Resource

View IT Resource Details and Parameters

You can view additional information about this IT resource :

IT Resource Name OPAMServer
IT Resource Type OPAM Server

Parameter	Value
Host	localhost
Password	*****
Port	18102
Username	apacheopamadmin

[Back to Search Results](#)

Check Schedule Job

Job Information

Job Name: OPAM Catalog Synchronization
 Task: OPAM Catalog Synchronization
 * Start Date: April 15, 2014 8:03:57 PM (UTC+05:30) Calcutta - India Time (IT)
 * Retries: 5

Schedule Type: ☒ Periodic
☐ Cron
☐ Single
☐ No pre-defined schedule

Job Periodic Settings

Run every: 15 mins

Job Status

Current Status: Stopped
 Last Run Start: April 15, 2014 8:11:56 PM IST
 Last Run End: April 15, 2014 8:12:02 PM IST
 Next Scheduled Run: April 15, 2014 8:18:57 PM IST

Parameters

* OPAM Server ID Store IT Resource: Apache DS LDAP
 * OPAM Server IT Resource: OPAMServer

5. Create OPAM_TAGS - this is a UDF in the Catalog form

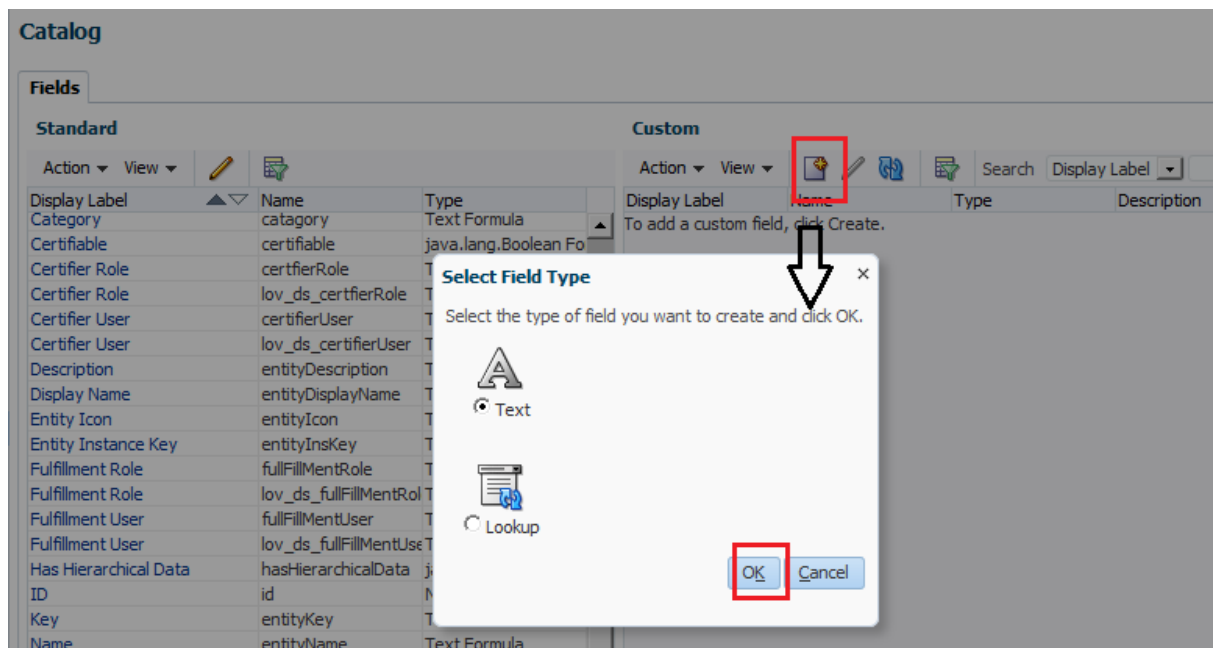
Create a sandbox and edit the Catalog Form in OIM

Manage Sandboxes x Manage Catalog x

Catalog [Import/Export](#)

Fields

Standard			Custom			
Action	View		Action	View	Search	Display Label
Display Label		Name	Display Label		Name	Type
Category		category	To add a custom field, click Create.			
Certifiable		certifiable			Type	Description
Certifier Role		certifierRole			Parent Field	
Certifier Role		lov_ds_certifierRole				
Certifier User		certifierUser				
Certifier User		lov_ds_certifierUser				
Description		entityDescription				
Display Name		entityDisplayName				
Entity Icon		entityIcon				
Entity Instance Key		entityInstKey				
Fulfillment Role		fulfillMentRole				
Fulfillment Role		lov_ds_fullfillMentRol				
Fulfillment User		fulfillMentUser				
Fulfillment User		lov_ds_fullfillMentUse				
Has Hierarchical Data		hasHierarchicalData				
ID		id				
Key		entityKey				



Appearance

* Display Label

Display Width Characters

Each field requires a unique name in the system. Name and description are for internal use only, and are never displayed to your users.

* Name	OPAM_TAGS
Description	OPAM metadata tags

☒ Searchable

Enter the value you want to set for the field when an object is created. Select Expression if you want to set the default dynamically.

 Certifiable

Catalog

Import/Export

Fields

Standard

Action	View		
Display Label	Name	Type	
Certifier User	certifierUser	Text Formula	
Description	entityDescription	Text Formula	
Display Name	entityDisplayName	Text Formula	
Entity Icon	entityIcon	Text Formula	
Entity Instance Key	entityInstKey	Text Formula	
Key	entityKey	Text Formula	
Name	entityName	Text Formula	
Type	entityType	Text Formula	
Taskflow ID	formid	Text Formula	
Fulfillment Role	fulfillMentRole	Text Formula	
Fulfillment User	fulfillMentUser	Text Formula	
Has Hierarchical Data	hasHierarchicalData	java.lang.Boolean Formula	
ID	id	Number Formula	

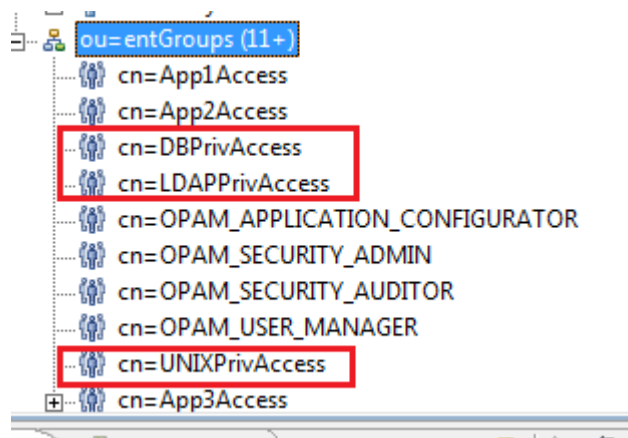
Custom

Action	View			
Display Label	Name	Type	Description	Parent Field
OPAM tags	OPAM_TAGS	Text	OPAM metadata tags	

6. Create groups in your LDAP server

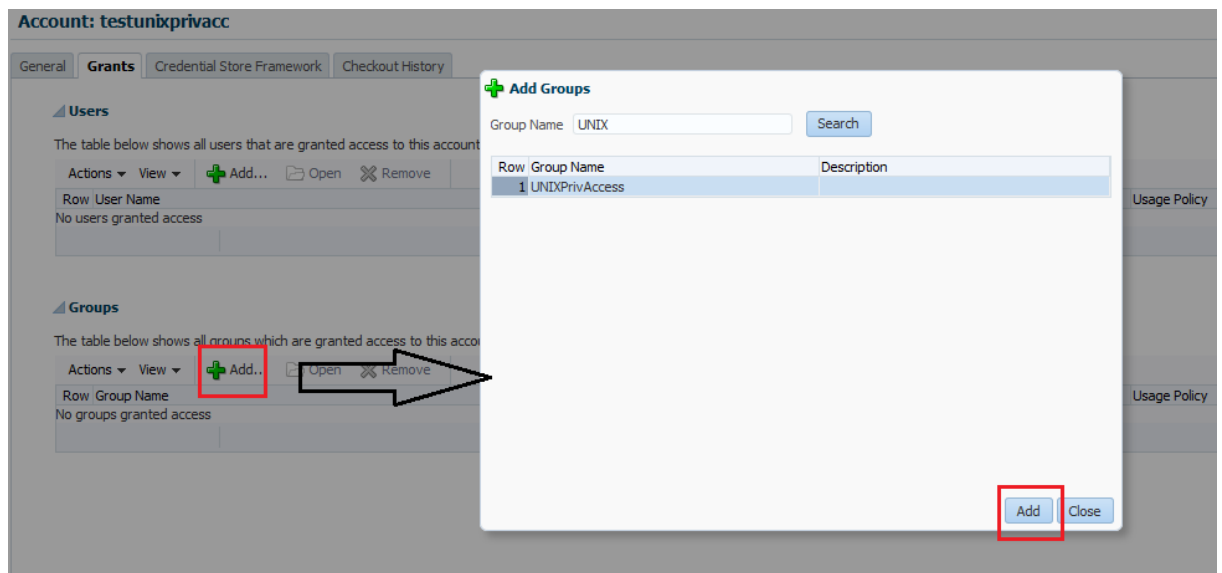
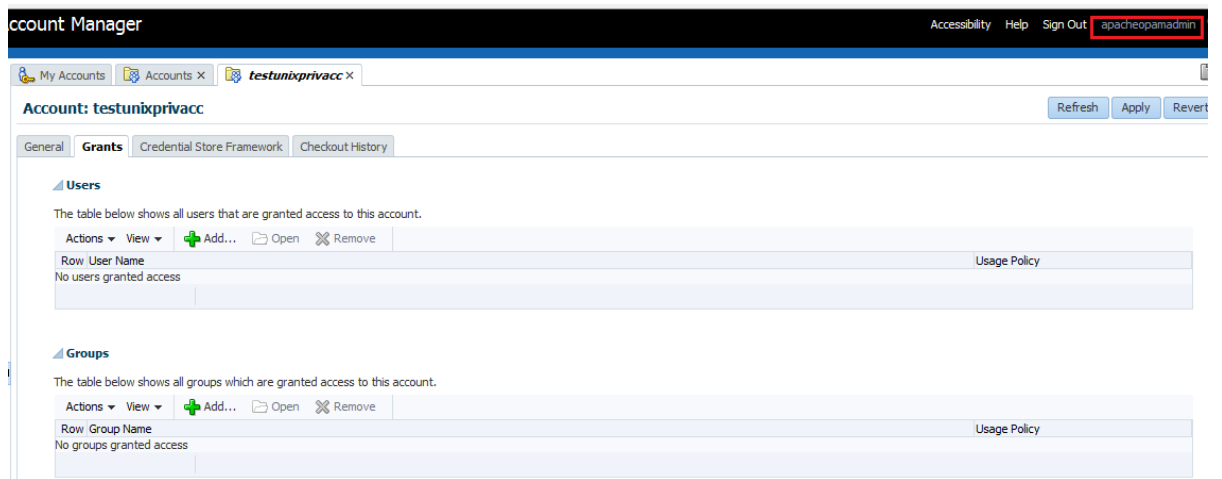
These groups would be configure in OPAM to manage access to privileged accounts and targets

Groups for LDAP, DB and UNI privilege accounts



7. Assign Grants to the privilege accounts based on groups

Log into OPAM as admin



+

Add Groups

Group Name

UNIX

Search

✓

Selected group(s) added successfully.

Row	Group Name	Description
1	UNIXPrivAccess	

Add

Close

Account: testunixprivacc

Refresh Apply Revert

General

Grants

Credential Store Framework

Checkout History

Users

The table below shows all users that are granted access to this account.

Actions

View

+

Add...

Open

Remove

Row	User Name	Usage Policy
No users granted access		

Groups

The table below shows all groups which are granted access to this account.

Actions

View

+

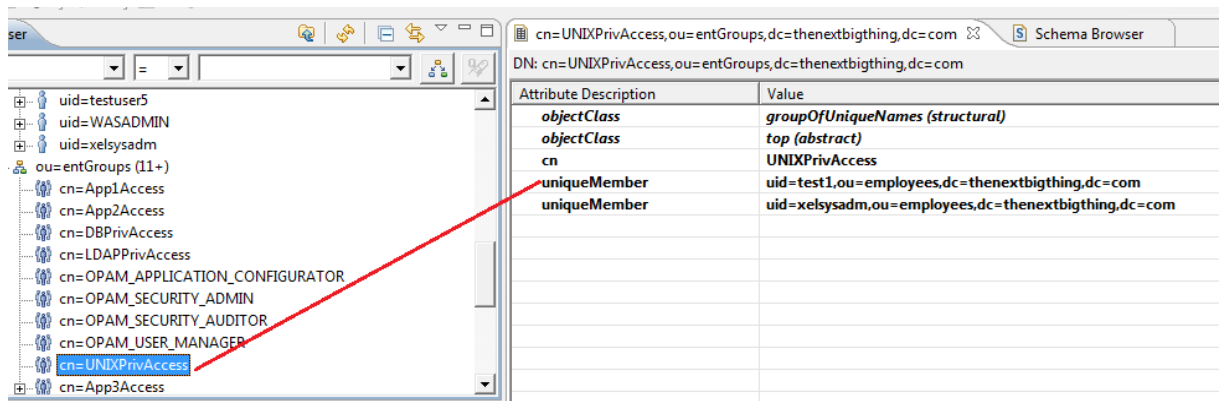
Add...

Open

Remove

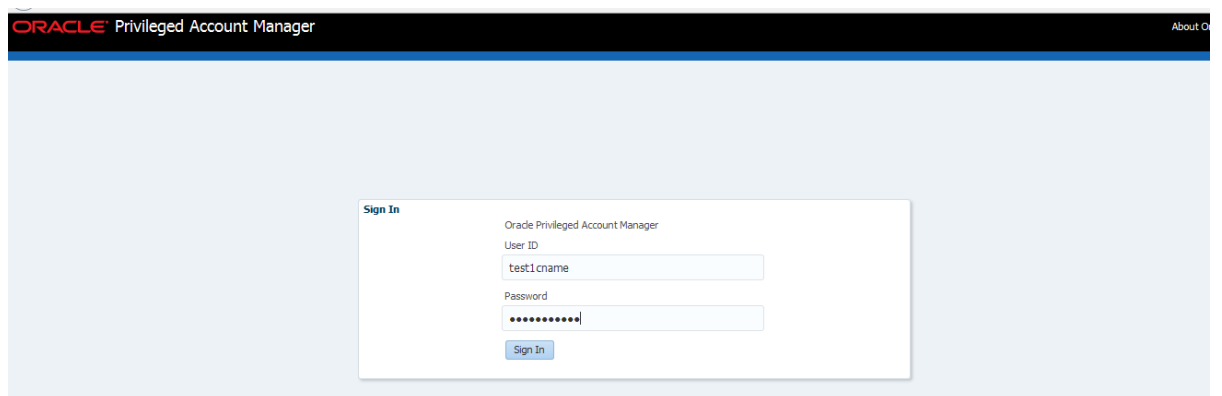
Row	Group Name	Usage Policy
1	UNIXPrivAccess	Default Usage Policy

- Log into OPAM as an end user who is a member of the Group configured above and see if he able to check out the UNIX account



New Delete		Showing 21 to 28 of 28 Previous	
<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	opamenduser1	End user of OPAM	DefaultAuthenticator
<input type="checkbox"/>	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
<input type="checkbox"/>	test1cname		LDAPAuthenticationProvider
<input type="checkbox"/>	testuser4_cn		LDAPAuthenticationProvider
<input type="checkbox"/>	testuser5_cm		LDAPAuthenticationProvider
<input type="checkbox"/>	wasadmin		LDAPAuthenticationProvider
<input type="checkbox"/>	weblogic	This user is the default administrator.	DefaultAuthenticator
<input type="checkbox"/>	xelsysadm		LDAPAuthenticationProvider

We'll use the above user since he is a member of the UNIXAccess group in LDAP



He has access to UNIX privileged account

My Accounts

Search Accounts

Account Name Domain
Target Type All Description
Target Name

Search Results

Actions View

Row	Account Name	Target Name	Target Type	Domain	Description
1	testunixprivacc	Local OEL Box	unix	testdomain	

Search Results

Actions View

Row	Account Name
1	testunixprivacc

☒ **Check-Out Account**

Account Name testunixprivacc
Target Name Local OEL Box
Justification

Let's confirm if it's checked out

My Accounts | My Checkouts x

My Checkouts

The table below shows all accounts which are currently checked out.

Actions	View	Check In	Show Password	Refresh					
Row	Account Name	Target Name	Target Type	Checkout Type	Domain	Expiration Date			
1	testunixprivacc	Local OEL Box	unix	password	testdomain	4/20/2014 9:06 PM			

We can safely check it in back again

My Checkouts

The table below shows all accounts which are currently checked out.

Actions	View	Check In	Show Password	Refresh		
Row	Account Name	Target Name	Target Type	Checkout Type	Domain	Expiration Date
1	testunixprivacc	Local OEL Box	unix	password	testdomain	4/20/2014 9:06 PM

Check-in Accounts

Click Check In to check-in the following account(s):

Row	Account Name	Target Name
1	testunixprivacc	Local OEL Box

Check In Cancel

Checked back in

My Checkouts

The table below shows all accounts which are currently checked out.

Actions	View	Check In	Show Password	Refresh					
Row	Account Name	Target Name	Target Type	Checkout Type	Domain	Expiration Date			
No checked-out accounts found.									

The same process is applicable for any Target/account - DB, LDAP etc